

**JC05 Rec'd PCT/PTO 12 OCT 2005**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

:

**10/552586**

Masato YAMAMICHI et al.

:

**Mail Stop: PCT**

Serial No. NEW

:

Attorney Docket No. 2005\_1537A

Filed October 12, 2005

:

PARAMETER GENERATION APPARATUS,  
ENCRYPTION SYSTEM, DECRYPTION  
SYSTEM, ENCRYPTION APPARATUS,  
DECRYPTION APPARATUS, ENCRYPTION  
METHOD, DECRYPTION METHOD, AND  
PROGRAM THEREOF

**[Corresponding to PCT/JP2004/005528**

**Filed April 14, 2004]**

**INFORMATION DISCLOSURE STATEMENT**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

Pursuant to the provisions of 37 CFR 1.56, 1.97 and 1.98, Applicants request consideration of the references listed on attached form PTO-1449 and any additional information identified below in paragraph 3. A legible copy of each reference listed on the Form PTO-1449 is enclosed, except a copy is not provided for:

- ☐ each U.S. Patent and U.S. Patent application publication;
- ☐ each reference previously cited in the international application  
PCT/\_\_\_\_\_; and/or
- ☐ each reference previously cited in prior parent application Serial No.  
\_\_\_\_\_.

1a. ☒ This Information Disclosure Statement is submitted:

ATTACHMENT C

within three months of the filing date (or of entry into the National Stage) of the above-entitled application, or

before the mailing of a first Office Action on the merits or the mailing of a first Office Action after the filing of an RCE,

**and thus no certification and/or fee is required.**

1b. ☐ This Information Disclosure Statement is submitted

after the events of above paragraph 1a and prior to the mailing date of a final Office Action or a Notice of Allowance or an action which otherwise closes prosecution in the application, and thus:

(1) ☐ the certification of paragraph 2 below is provided, **or**

(2) ☐ the fee of \$180.00 specified in 37 CFR 1.17(p) is enclosed.

1c. ☐ This Information Disclosure Statement is submitted:

after the mailing date of a final Office Action or Notice of Allowance or action which otherwise closes prosecution in the application, and prior to payment of the issue fee, and thus:

**the certification of paragraph 2 below is provided, and**

**the fee of \$180.00 specified in 37 CFR 1.17(p) is enclosed.**

2. It is hereby certified

a. ☐ that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Statement, or

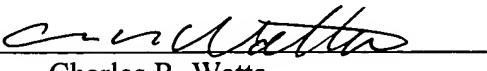
b. ☐ that no item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the person signing the certification

after making reasonable inquiry, was known to any individual designated in §1.56(c) more than three months prior to the filing of the Statement.

3. ☐ Consideration of the following list of additional information (including any copending or abandoned U.S. application, prior uses and/or sales, etc.) is requested.
4. For each non-English language reference listed on the attached form PTO-1449, reference is made to:
- a. ☐ a full or partial English language translation submitted herewith,
  - b. ☐ a foreign patent office search report (in the English language) submitted herewith,
  - c. ☒ the concise explanation contained in the specification of the present application at pages 1-5,
  - d. ☐ the concise explanation set forth in the attached English language abstract,
  - e. ☐ the concise explanation set forth below or on a separate sheet attached to the reference:
5. ☒ the International Search Report citing one or more of the references is enclosed.

Respectfully submitted,

Masato YAMAMICHI et al.

By   
Charles R. Watts  
Registration No. 33,142  
Attorney for Applicants

CRW/asd  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
October 12, 2005

FORM PTO 1449 (modified)

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICELIST OF REFERENCES CITED BY APPLICANT(S)  
(Use several sheets if necessary)

Date Submitted to PTO: October 12, 2005

ATTY DOCKET NO.  
2005\_1537ASERIAL NO.  
NEW PTO 12 OCT 2005APPLICANT  
Masato YAMAMICHI et al.

10/552586

FILING DATE  
October 12, 2005

GROUP

## U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						

## FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO
	AF						
	AG						
	AH						

## OTHER DOCUMENT(S) (Including Author, Title, Date, Pertinent Pages, Etc.)

	AI	J. Silverman, "Wraps, Gaps, and Lattice Constants", NTRU Cryptosystems Technical Report, Report 11, 'online! March 15, 2001, pp. 1-6, XP002288211, retrieved from the Internet: URL: <a href="http://www.ntru.com/cryptolab/pdf/NTRUTech011_v2_pdf">http://www.ntru.com/cryptolab/pdf/NTRUTech011_v2_pdf</a> 'retrieved on July 12, 2004
	AJ	J.H. Silverman et al., NTRU Cryptosystems Technical Report - Report #18, Version 1: "Estimating Description Failure Probabilities for NTRUEncrypt", 'online! June 2003), pp. 1-17, XP002288212, retrieved from the internet: URL: <a href="http://www.ntru.com/cryptolab/pdf/NTRUTech018.pdf">http://www.ntru.com/cryptolab/pdf/NTRUTech018.pdf</a> 'retrieved on 7-12-2004
	AK	N. Howgrave-Graham et al., "The Impact of Description Failures on the Security of NTRU Encryption", In-Proc. Crypto 2003, Santa Barbara, USA, 2003, 'online! August 2004, pp. 1-22, XP002288213, retrieved from the internet: URL: <a href="http://www.ntru.com/cryptolab/pdf/cr03_ntru.pdf">http://www.ntru.com/cryptolab/pdf/cr03_ntru.pdf</a> 'retrieved on 7-12-2004
	AL	J.H. Silverman: "Dimension-Reduced Lattices Zero-Forced Lattices and the NTRU Public Key Cryptosystem," NTRU Cryptosystems Technical Report, Report 13, 'Online!, March 9, 1999, pp. 1-14, XP002288214, retrieved from the internet: URL: <a href="http://www.ntru.com/cryptolab/pdf/NTRUTech013.pdf">http://www.ntru.com/cryptolab/pdf/NTRUTech013.pdf</a> 'retrieved on 7-12-2004
	AM	J. Hoffstein et al., "NTRU: A Ring-Based Public Key Cryptosystem", lecture notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998
	AN	J. Silverman, "NTRU Cryptosystems Technical Report #012, Version 1", "Estimated Breaking Times for NTRU Lattices", 'Online!, March 9, 1999, pp. 1-7, retrieved from the internet: URL: <a href="http://www.ntru.com/cryptolab/pdf/NTRUTech012.pdf">http://www.ntru.com/cryptolab/pdf/NTRUTech012.pdf</a> 'retrieved on 2-18, 2003

EXAMINER

DATE CONSIDERED

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include cop. this form with next communication to applicant.